Leistungsbeschreibung & zusätzliche Bedingungen TeleSec IDKey µSD

Version: 1.0

Stand: 01.09.2018

Impressum

Herausgeber

T-Systems International GmbH

Hahnstraße 43d

60528 Frankfurt am Main

WEEE-Reg.-Nr. DE50335567

nachfolgend – Telekom – genannt

www.t-systems.de/pflichtangaben

INHALT

EINLEITUNG

Bei IDKey µSD handelt es sich um einen NICHT personifizierte Kryptochip mit dem T-Systems eigenem Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System), optimiert für die Verwendung im Windows-Umfeld.

IDKey µSD unterstützt das Windows Identity Life Cycle Management (ILM) und kann hiermit für Zugangsberechtigungen zu Personal Computern, Servern und Netzen eingesetzt werden. Außerdem dient IDKey µSD der Integritätssicherung und ermöglicht die Ver- und Entschlüsselung beliebiger Dateien. Weitere Applikationen können zusätzlich auf dem Chip implementiert werden.

1 LEISTUNGEN DER TELEKOM

1.1 Bereitstellung

Die Telekom erbringt folgende Leistung:

1. Lieferung der produktrelevanten Dokumentation
2. Lieferung der TeleSec IDKey µSD TCOS 3.0

System-Voraussetzungen

- Kartenlesegerät
- PC mit Software zur Ansteuerung der verfügbaren Applikationen
- Bei Einsatz von Einmal-Passwörtern Teilnahme an der Dienstleistung OTP

Typbezeichnung:

µSD Format	Dual Interface	Typbezeichnung
x		736/080 µSD V30-2GB

1.2 Funktionen

Bei IDKey µSD handelt es sich um einen NICHT personifizierten Kryptochip mit dem Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System).

IDKey µSD enthält bei Auslieferung verschiedene asymmetrische Schlüsselpaare und symmetrische Schlüssel. Die kryptographischen Schlüssel sind in Verbindung mit physikalischen Kartennummern eindeutig. Es existieren keine Kopien der privaten Schlüssel.

IDKey µSD wird im sogenannten NullPIN-Status ausgeliefert. Die NullPIN sichert die Unversehrtheit des Produkts und erspart den Versand eines PIN-Briefes. Vor einer Nutzung von IDKey wird die NullPIN durch eine persönliche PIN ersetzt.

Eine Zuordnung zu bestimmten Personen oder Systemen (Personalisierung) wird nach Auslieferung im Kundenumfeld vorgenommen.

IDKey µSD enthält bei der Auslieferung die folgenden Standardapplikationen:

ILM (Identity Life Cycle Management):
Entschlüsselung,
fortgeschrittene Signatur,
Authentikation.

Diese Applikation kann z.B. mit dem TCOS 3.0 Card Module über den Microsoft BaseCSP in das Microsoft ILM (Identity Life Cycle Management) integriert werden. Eine Nutzung vergleichbar zur NetKey-Applikation der NetKey 3.0 ist ebenfalls möglich.

OneTimePass (OTP): Erzeugung von Einmalpasswörtern.

Gleitzeit (GLAZ): Gleitzeiterfassung

Zutritt (ZTRT): Sicherung von Gebäudeteilen

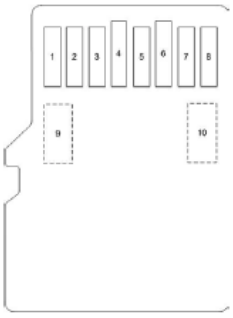
Leistungsmerkmale der IDKey µSD-Card

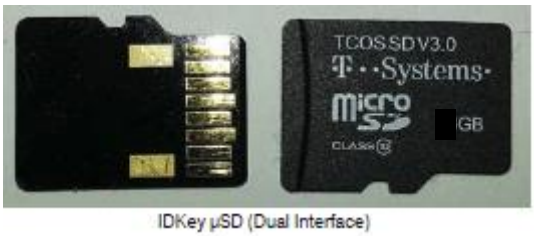
- Intelligente Prozessorchipkarte mit dem eigens hierfür von der T-Systems entwickelten Chipkarten-Betriebssystem TCOS, RSA2048 Bit Schlüssellänge, DES, 3-DES und IDEA
- Einfache Integration der IDKey µSD in das Microsoft Betriebssystem Windows (2000,XP,Vista,W7)
- Identity Life Cycle Management (ILM)
- Direkt Integriert in Microsoft Standart-Anwendungen (z.B. Outlook, Internet Explorere, Word) über Microsoft-Crypto-API bzw. Microsoft Crypto Next Generation.
- Verwendbar auch unter Linux
- Fortgeschrittene Signatur
- Entschlüsselung von Authentifikation
- Zugangsschutz für Firewalls, Router, Webserver, Internet Service-Provider, sicherer Domain-Login
- Mit sech2048 Schlüsselpaaren aus T-Systems Trustcenter vorpersonalisiert
- Vorbereitet für Key-Recovery
- Unterstützung des Challenge-Response-Verfahrens
- Authentifizierung der Endkunden durch das Trustcenter der DTAG bei Nutzung der Dienstleistung OTP.
- Zutritt (ZTRT) – Sicherung von Gebäudeteilen
- Gleitzeit (GLAZ)
- OneTimePass (OTP) – Erzeugung von Einmal-Passwörtern
- Verfügbarkeit umfassender Dokumentationen
- Verfügbarkeit von Schnittstellen-Software
    - TCOS-Cardmodul zum Microsoft SmartCard BaseCSP
    - PKCS#11-Modul für Windows und Linux

Bauformen

TCOS µSD V3.0 – 2GB

Micro SD Karte mit 2GB Flasch Speicher und integriertem TCOS Smartcard Chip
ISO 14443 Kommunikation ist über eine an Pin 9 und 10 angeschlossene Antenne möglich.





IDKey µSD (Dual Interface)

Technische Daten

Betriebssystem:	**TCOS 3.02**
Befehlssatz:	gemäß ISO 7816
Typbezeichnung:	736
Kartennummer:	89 49 01736 xxxxxxxxx x
Protokoll:	T=1 nach ISO 7816-3
	T=CL nach ISO 14443 (bei DI-Karten)
Chiptyp:	NXP P5CD080,
	evaluiert nach CC EAL 5+
Speichergröße:	insgesamt: 80 kByte (EEPROM)
Schlüssellänge:	RSA bis max. 2048 bit
Algorithmen:	DES, 3DES, RSA
Chaining	ECB, CBC

1.3 Optionale Leistungen

- Weitere Varianten des Produkts auf Anfrage